# Anforderungen an eine leistungsfähige Interne Revision in einem Kreditinstitut aus Sicht von MC-Banksoftware - Version 2

Dieser Artikel beschäftigt sich mit wesentlichen Anforderungen an eine Interne Revision. Hierbei wird auf die eigenen Erfahrungen und Aktivitäten als Revisor reflektiert und in nachstehenden Aussagen auf wesentliche Anforderungen an eine wirksame Interne Revision aus eigener Sicht verwiesen.

## 1. Die Interne Revision bewegt sich im Rahmen ihrer Handlungen auf Basis strategischen Vorgaben.

Grundlage für Ihre Tätigkeit sind strategische Festlegungen im Rahmen von Strategien. Hierbei berücksichtigt die Interne Revision die Aussagen, Ziele und Maßnahmen der Geschäfts- und Risikostrategien der Bank. Die IR formuliert eine Revisions-, Prüfungs- , Projekt- und gggfls. Eine Beratungsstrategie. Die Prüfungsstrategie teilt sich in eine Gesamtbankprüfungsstrategie und in Teilstrategien für die wesentlichen Prüfungsfelder auf.Auf eine prozessorientierte Betrachtung ist dabei zu achten. AT 4.3.1 Tz 2 wird dabei berücksichtigt. Die Strategien der IR sind keine Strategien im Sinne der MaRisk (AT 4.2 der MaRisk).

## 2. Die Interne Revision muss prozessorientiert ausgerichtet werden. Hierbei wird zwischen Haupt- und Teilprozessen unterschieden.

Es ergeben sich nachstehende wesentliche Hauptprozesse der Internen Revision:

**Aufgabenbezogene Prozesse**

- Prüfungsprozesse
- Projektbegleitungsprozesse
- Beratungsprozesse
- Informationstransferprozesse
- Revisionsresearchprozesse

**Überprüfungsprozesse**

- Qualitätsmanagementprozesse

**Organisationsprozesse**

- Revisionsorganisationsprozesse

Im Rahmen einer weiteren Prozessbetrachtung ergeben sich aus obigen Prozessbereichen auch entsprechend der MaRisk nachstehende Prozesstypen:Leitungs-, Steuerungs- und Kontrollprozesse der IR ( siehe auch AT1 der MaRisk)

### 3. Die Interne Revision muss sich dynamisch auf die wechselnden Anforderungen einstellen. Statische Betrachtungen sind einer fortlaufenden Bewertung zu unterziehen.

Zum Jahresende wird in der Regel für das Folgejahr ein neues Prüfungsprogramm erstellt. Dies erfolgt durch Formulierung einer Prüfungsstrategie und der Fortschreibung eines Mehrjahresplanes. Die Prüfungen werden in der Folgezeit abgearbeitet. Zu Beginn der Prüfung wird dann der zurückliegende Zeitraum von der Erstellung der Prüfungsstrategie bis zur Prüfung bewertet. Dieser Ansatz greift aber zu kurz, da hier zwei statische Betrachtungen erfolgen. Der Ansatz muss vielmehr dynamisch sein. Das stichtagsbezogen erstellte Prüfungsprogramm ist nach Erstellung fortlaufend weiterzuentwickeln. Im Rahmen eines „Revisionsradars“ oder „Revisionsresearch“ sind für die wesentlichen Prüfungsfelder fortlaufend Erkenntnisse und Informationen zu sammeln und zu bewerten, ob der bisherige Prüfungsansatz noch risikoangemessen ist. Die Beteiligung der Internen Revision und anderer „Besonderer Funktionen“ ergeben sich z.B, aus dem AT 8.1 und 8.2 der MaRisk.Ist dies nicht der Fall, ist das Prüfungsprogramm, d. h. hier die Strategie und der Prüfungsplan abzuändern. Erfolgt anlassbezogen durch die Bank, z.B. entsprechend der MaRisk eine neue Risikotragfähigkeitsberechnung, muss dies zu entsprechenden Neubewertungen der risikoorientierten Prüfungsplanung führen. Letztlich unterliegt der Prüfungsplan einem permanenten Veränderungsprozess mit allen sich daraus ergebenen Konsequenzen (z.B. Besprechung notwendiger Veränderungen im Rahmen der Governanceprozesse).

### 4. Die Interne Revision muss ihren Anteil an vorausschauenden Betrachtungen erhöhen.

Neben der Prüfung muss der Anteil der Begleitung von Veränderungsprozessen in der Bank erhöht werden. Dies erfolgt durch Projektbegleitungen und u.U. durch Beratungstätigkeiten. Die Grundsätze der Internen Revision (z.B. Unabhängigkeit) müssen dabei beachtet werden. Im Rahmen dynamischer Betrachtungen sind wesentliche Projekte zwingend zu begleiten, da diese zu Veränderungen im Risikomanagement und dem Internen Kontrollsystem führen können. Ich sehe hier auch einen präventiven Ansatz durch die Interne Revision.

Ob der Anteil der Prüfungen abnimmt, ist risikoorientiert zu entscheiden. Hier darf es nicht wechselseitig zu Risiken kommen, indem die ex post oder ex ante Betrachtung zu kurz kommt.

### 5. Die Interne Revision muss im Rahmen ihrer Prüfung prozessorientiert vorgehen.

Die prozessorientierte Betrachtung erhöht die Granularität der Prüfung. Mögliche Schnittstellenprobleme werden erkannt und IKS ordnende Systeme, die im ersten Moment nicht als Prüfgegenstand erkannt werden- aber wesentlich sind- werden so einbezogen.

Hierdurch werden u. U. weitere wichtige qualitätsoptimierende Maßnahmen ausgelöst.

Beispiel:
Bei der Betrachtung eines Bearbeitungsprozesses wird auch auf die im Rahmen der Bearbeitung eingesetzten Systeme (AT 7.2 der MaRisk – Frage nach Test- und Freigabeverfahren eventueller Excelsheets) und auf die Ablage dieser Dateien (LAN Rechte und notwendige Funktionstrennungen nach MaRisk) reflektiert. Die Prüfungsfragen beziehen sich dann nicht nur auf den Prüfungsgegenstand, sondern auch auf die vorgenannten Punkte, da sie ja Bearbeitungsschritte darstellen.

## 6. Die Interne Revision benötigt eine Art „Research“ oder „Radar“, der permanent mögliche wesentliche „Risikotreiber „ untersucht.

Vorgenannte Darstellung greift sicher noch zu kurz. Kern dieser Anforderung ist eine permanente Informationsbeschaffung und Auswertung wesentlicher Aktivitäten und Prozesse der Bank.

Dies geschieht u.a. durch die Auswertung erhaltender Risikoberichte (nach MaRisk) und einzelner Datenanalysen, um mögliche Risikotreiber zu erkennen. Dies stellt keine „Konkurrenz“ im Rahmen produktiver Risikoanalysen dar (z.B. Darstellung von Risikokonzentrationen im Adressrisikobericht), die Aufgabe der Bank sind. Vielmehr sollen aus der Analyse laufender Prozessen, Erkenntnisse für die eigene Revisionstätigkeit erfolgen.

## 7. Die Interne Revision bedarf angemessener Organisationsprozesse.

Rahmenbedingungen sind als organisatorische Regelung für eine Revision häufig anzutreffen. Daneben bestehen in der Regel eine Arbeitsanweisung, ein Ratingverfahren, Wesentlichkeitsgrenzen und Strategien. In der gelebten Praxis bestehen daneben Prüfungsberichte, ein Jahresbericht und entsprechende IT-Systeme für die IR. Hier gibt es sicher noch weitere Punkte, die aufgezählt werden können.

Der Betrachtungshorizont dieser Anforderung beschäftigt sich mit dem „IKS“ innerhalb der Internen Revision. Im ersten Moment vielleicht widersinnig.

Die Interne Revision muss im Rahmen ihrer Aktivitäten auch die Anforderungen der MaRisk erfüllen. Zu nennen sind hier AT 5 und AT 6 der MaRisk. Kontrollprozesse innerhalb der Prüfungen und entsprechende Dokumentationen sind entsprechend anzuweisen.

## 8. Die Interne Revision bedarf granularer Ratingsyteme.

In der Regel besteht in der IR eine Ratingsystematik von 1 bis 5. Es wird von geringen, unwesentlichen, bemerkenswerten, von wesentlichen Mängeln,... gesprochen.
Dies erscheint zu undifferenziert. Meines Erachtens werden unterschiedliche Ratingsysteme benötigt.

Ratingverfahren für Prüfungen der Aufbau- und Ablauforganisation
Ratingverfahren für Funktionsprüfungen
Ratingverfahren für aussagebezogene Prüfungshandlungen.

Die Ausgestaltung der Ratingverfahren ist unterschiedlich und muss die verschiedenen Anforderungen berücksichtigen. Die Begriffe gering, unwesentlich oder schwerwiegend sind genau zu definieren und mit z.B. dem „Versagen“ von Schlüsselprozessen zu unterlegen.

Anders ausgedrückt, die Ratingsystematik muss erkennen lassen, wie z.B. ein Verstoß nach AT 7.2 der MaRisk zu gewichten ist, wenn z.B. die Schlüsselprozesse zum Test- und Freigabeverfahren im Rahmen des IT-Sicherheitsmanagements nicht gegriffen haben.

Zusätzlich ist festzulegen, was eine Feststellung ist. Es ist festzulegen, was ein „Fehler“ ist. Gleichzeitig ist dieser zu gewichten. Es kann hier entgegnet werden : “ Jede Abweichung von einer gesetzliche Norm oder jede Abweichung einer Regelung ist ein Fehler“. Aber erst in der Gewichtung erfolgt ein Bezug zu einer möglichen Wesentlichkeit.

Hierbei ist auch zu definieren, was eine Empfehlung ist.

Grundsatz der IR muss es sein Feststellungen transparent und klar zu definieren. Die verletzte Norm ist immer anzugeben.

## 9. Die Interne Revision ist Teil des Risikomanagements. Deren Systeme d.h. eingesetzten Methoden und Verfahren sind regelmäßig und anlassbezogen zu überprüfen.

Die Interne Revision muss ihre Prüfungen risikoorientiert ausrichten. Insoweit kommt den wesentlichen Risikoarten in der Prüfung ein besonderer Stellenwert zu. Unter Risikogesichtspunkten kommt der Prüfung der wesentlichen Risikoarten und deren Steuerung somit eine wesentliche Bedeutung zu. Genügend Kapazitäten sind zur Verfügung zu stellen.

Da innerhalb der vorgenannten – und auch auch aller anderer Prozesse- Informationstechnologie zum Einsatz kommt, sind die Prozesse im Rahmen von AT 7.2 auch von wesentlicher Bedeutung. Da hier auch operationelle Risiken auftreten können ist zusätzlich eine wesentliche Risikoart betroffen.

Die weiteren Risikomanagementprozesse nach AT der MaRisk (z.B. Notfallprozesse, Prozesse nach AT 5 und 6) sind weiterhin wesentlicher Betrachtungsgegenstand.

Die einzelnen Risikomanagementprozesse werden über Methoden und Verfahren abgebildet. Wesentliche Methoden und Verfahren sind dabei zu validieren. Diese sind somit auch wesentliche Prüfungsbereiche der Internen Revision.

**Michael Claaßen**